数理解析研究所講究録
1038巻 1998年 244-254

Risa/Asir による modular polynomial の計算

伊豆哲也 (富士通研究所HPC研究センター)
izu@flab.fujitsu.co.jp

Abstract. 楕円曲線上の有理点の個数を数えるSchoofアルゴリズムの改良において, モジュラー多項式 $\Phi_l(X,j)$ が大きな役割を果たすことが指摘されているが, 大きな l に対する具体的な計算例はあまり見られない. そこで数式処理システム Risa/Asir を用いて, $l=97$ までのモジュラー多項式を求めたので, その計算結果について報告する.

1. はじめに

次世代の公開鍵暗号として楕円曲線暗号が注目されている. 有限体 F 上で定義された楕円曲線の F 有理点は加法群の構造を持ち, 楕円曲線暗号はこの群における離散対数問題を利用している. したがって暗号を実現させる立場からは, この有理点の個数 (群位数) は暗号の安全性に直結する重要なパラメータであり, 高速に計算できなくてはならない.

Schoofは $F=GF(p)$ (p は素数) の場合における群位数を計算する多項式時間アルゴリズムを考案した [Sc85] が, その計算量は $O(\log^8 p)$ であり, 実用性は低かった. しかしAtkin,Elkiesらによる本質的な改良により, 計算量は $O(\log^6 p)$ にまで低下させた [Sc95]. 彼らの改良において本質的な役割を果たしたのがモジュラー多項式 (modular polynomial) である.

モジュラー多項式とは, 楕円モジュラー関数 $j(z)$ と素数 l に対して,

$$\Phi_l(X,j)=\Big(X-j(lz)\Big)\prod_{k=0}^{l-1}\left(X-j\Big(\frac{z+k}{l}\Big)\right)$$

によって定義される多項式をいう. $\Phi_l(X,j)$ は整数係数であるが, l が大きくなるにつれてその係数は巨大になり, 計算するのが非常に困難となる. 具体的な計算結果としては, 筆者の知る限り $l=53$ までしか求められていない [Ito95].

筆者の属するグループではSchoof,Elkies,Atkinらによる群位数計算アルゴリズムを数式処理システム Risa/Asir によって実現させている [Kog97]. その計算において, 大きな素数 l に対するモジュラー多項式 $\Phi_l(X,j)$ が必要となり, 実際に $l=97$ までのモジュラー多項式を計算した. 以下ではその計算結果について報告する.

2. 定義など

説明で必要な用語などを定義する. 詳細な定義・性質については [La87] を参照されたい.

2.1. 楕円モジュラー関数

複素上半平面の点 z に対し $q = e^{2\pi z\sqrt{-1}}$ と定め, z の関数と q の関数を同一視する. $\sigma_k(n)$ で n の約数の k 乗和 $\sigma_k(n) = \sum_{d|n} d^k$ を表すことにして, 関数

$$E_4 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$$

を定める. このとき, 楕円モジュラー関数 $j(q)$ は次式で定義される:

$$j(q) = j(z) = \frac{E_4^3}{\Delta}.$$

$j(q)$ は q の有理関数として表され, 具体的には

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots.$$

となる. 初項以外の項は整数係数であり,

$$j(q) - \frac{1}{q} = \sum_{n=0}^{\infty} c_n q^n \in Z[[q]]$$

となる. $\{c_n\}$ は正の値をとりながら単調増加していく.

2.2. モジュラー多項式

楕円モジュラー関数 $j(z)$ と素数 l に対し, 次式で定義される多項式をモジュラー多項式という:

$$\begin{aligned}\Phi_l(X,j) &= \Big(X - j(lz)\Big)\prod_{k=0}^{l-1}\left(X - j\Big(\frac{z+k}{l}\Big)\right)\\ &= X^{l+1} + j^{l+1} + \sum_{m,n=0}^{l} a_{mn}X^m j^n.\end{aligned}$$

$\Phi_l(X,j)$ は X, j に関する二変数の整数係数多項式であり, X, j の対称式となる.

モジュラー多項式は X の一変数多項式

$$\Phi_l(X,j) = X^{l+1} + \sum_{k=1}^{l+1}(-1)^k s_k(j)X^{l-k+1}$$

と見なすこともできる. ここで係数 $s_k(j)$ は j の整数係数多項式である. したがって $\Phi_l(X,j)$ を求めるには, 各係数 $s_k(j)$ が求められればよい. なお $s_k(j)$ は,

$$J_l = \left\{j(lz), j\Big(\frac{z}{l}\Big), j\Big(\frac{z+1}{l}\Big), \ldots, j\Big(\frac{z+l-1}{l}\Big)\right\}$$

の対称式として表される. 小さな l に対する具体的な数値例を付録に添付しておく.

3. 計算アルゴリズム

以下では, $j(q)$ が必要な次数まで計算できていると仮定する.

3.1. モジュラー多項式の計算 (1)〜通常の方法

素朴なアルゴリズムとして, 定義式に従って計算していく方法が考えられる.

まず J_l の各元を求める. $j(z)$ は求められているので, z に順番に代入していくことで,

$$j(lz) = \frac{1}{q^l} + c_0 + c_1 q^l + \dots$$
$$j\left(\frac{z+k}{l}\right) = \frac{1}{\zeta^k q^{1/l}} + c_0 + c_1 \zeta^k q^{1/l} + \dots$$

が得られる (ただし $0 \le k \le l-1$, ζ は 1 の l 乗根).

各 s_k はこれらの式の組み合わせから計算されるので, s_k は q の有理関数で表される. したがって j の多項式 $s_k(j)$ に変換しなければならない. しかし $s_k(j)$ は整数係数多項式になることがわかっているから, s_k の低次の項と $j(z)$ のべき乗から, 順に係数を合わせていけば良い. したがって s_k は定数項まで正しく求められている必要があるなお s_k に現れる q の最低次の項は $q^{-(l+1)}$ なので, $j(q)$ は $l(l+1)$ 次の項まで求められていれば良い.

このアルゴリズムでは 1 の l 乗根 ζ が必要になるが, Risa/Asir などの数式処理システムでは代数的数の扱いが可能であり, 実現は難しくないものの, 計算速度の低下を招いてしまう[1]. また $j(z)$ の係数の特徴により, 途中の計算での係数膨張が大きくなりすぎるという問題もあるため, 実用的ではない. 実験してみると, s_k を求める部分が律速段階となってしまう. 実際の計算では, l が 1 けたでないと Φ_l を求めるのが困難である.

3.2. モジュラー多項式の計算 (2)〜べき乗の利用

$s_k(j)$ が J_l の対称式で表されるので, 対称式に関する Newton 公式の利用による高速化が考えられる. 以下 [Ito95] にしたがってアルゴリズムの概要を述べる.

J_l の元のうち $j(lz)$ だけは他の元と性質が異なるので, 別に扱うほうが好ましい. そこで J_l から $j(lz)$ を除いた集合を

$$\overline{J}_l = \left\{ j\left(\frac{z}{l}\right), j\left(\frac{z+1}{l}\right), \dots, j\left(\frac{z+l-1}{l}\right) \right\}$$

とおく. また. $\overline{J}_l$ による基本対称式を

$$t_1 = \sum j\left(\frac{z+k}{l}\right)$$
$$t_2 = \sum j\left(\frac{z+k}{l}\right) j\left(\frac{z+k'}{l}\right)$$
$$\vdots$$
$$t_l = j\left(\frac{z}{l}\right) j\left(\frac{z+1}{l}\right) \cdots j\left(\frac{z+l-1}{l}\right)$$

---

[1] もっともここで必要となる代数構造は平易なので, 代数的数の使用を避けることが可能である.

とおく. ただし $t_0=1$, $t_{l+1}=0$ とする. このとき $\{s_k\}$ と $\{t_k\}$ の関係は

$$s_k = j(lz)\cdot t_{k-1} + t_k$$

となっている.

ここで $j(z)$ の r 乗を

$$j^r(z) = \sum_{n=-r}^{\infty} c_n^{(r)} q^n,$$

$\overline{J}_l$ の元たちの r 乗和 u_r を

$$u_r = \sum_{k=0}^{l-1} j^k\Big(\frac{z+k}{l}\Big) \quad (1 \le r \le l)$$

とおく. このとき以下の命題が成立する.

命題 1

$$u_r = l\sum_{n=0}^{\infty} c_{ln}^{(r)} q^n \quad (1 \le k \le l-1),$$
$$u_l = l\Big(\frac{1}{q} + \sum_{n=0}^{\infty} c_{ln}^{(l)} q^n\Big).$$

命題 2 (対称式に関する Newton 公式)

$$\begin{aligned} t_1 &= u_1, \\ t_2 &= -\frac{1}{2}(u_2 - t_1u_1), \\ t_3 &= \frac{1}{3}(u_3 - t_1u_2 + t_2u_1), \\ &\vdots \\ t_{l-1} &= -\frac{1}{l-1}(u_{l-1} - t_1u_{l-2} + \ldots - t_{l-2}u_1). \end{aligned}$$

実際の計算においては, $j(q)$ のべき乗 $j^r(q)$ $(r=1,2,\ldots,l+1)$, $\{u_r\}$, $\{t_k\}$, $\{s_k\}$, $\Phi_l(X,j)$ の順に計算していけば良いことがわかる. 最終的に j^{l+1} の係数が必要となるので, j は $l(l+1)$ 次まで必要となる.

4. 計算結果

われわれはべき乗を利用したアルゴリズムを用いて, $l=97$ までの 25 個のモジュラー多項式を求めた. 以下にその計算時間を示す[2]. ただし $j(q)$ はあらかじめ用意したデータを用いた. なおこれ以降の l に対しては並列計算を用いたため, 同じ尺度での計算時間を算出できなかった.

---

[2] 講演後にプログラム的な改良を加えた後の結果を示す.

l	計算時間 (秒)	l	計算時間 (秒)
2	0.05	37	1489
3	0.06	41	2981
5	0.13	43.	3941
7	0.35	47	6900
11	2.27	53	13602
13	4.72	59	28530
17	19.47	61	34789
19	31.28	67	63093
23	99.82	71	85282
29	369.5	73	103413
31	527.3		

(PentiumPro 200MHz,128MB RAM)

時間配分を考えると, 比率は l に依存していないので, 例えば $l = 73$ の場合で考える. 各段階の計算時間は次のようになる.

段階	$j^r(z)$	$\{u_k\}$	$\{t_k\}$	$\{s_k\}$	$\Phi_l(X, j)$
時間 (秒)	95048	84	8099	181	1
割合 (%)	(91.9)	(0.1)	(7.8)	(0.2)	(0.0)

表からわかる通り, 律速段階になっているのは $j(z)$ のべき乗計算であり, これは $l(l+1)$ 次の密で, しかも係数が膨大な多項式の乗法を繰り返し計算しているからであると思われる.

以上をふまえて計算の高速化を考える. まず効果が大きいのは乗法アルゴリズムそのものの改良であろう. 今回は Karatsuba 法を用いたが, l の大きさによっては FFT を用いることができるのかもしれないが, 今回は実験を行わなかった. これは今後の課題の一つである.

次にべき乗計算の効率化が挙げられる. そもそもべき乗のデータは上位互換, つまり例えば $l = 13$ の計算に使用したべき乗のデータは $l = 11$ の計算にも用いることができる, ので, 今回のように各 l に対してべき乗をいちいち計算するのは無駄が多い. したがってあらかじめ適当な大きさの自然数 n に対し, データ $\{j^i(q)\}$ $(i = 1, 2, \ldots, n)$ を用意しておけば, $l < n$ であるモジュラー多項式 $\Phi_l(X, j)$ の計算は簡単に実行できる. ここでべき乗計算は複数計算機を用いた並列計算が可能である. 確実な台数効果が見込めるので, 効果はかなり大きい[3].

5. まとめ

モジュラー多項式 $\Phi_l(X, j)$ の具体的な計算を, Risa/Asir を用いて $l = 97$ まで行った.

本稿を作成中に, 静岡大学の浅井哲也先生から Borcherds 積を利用した計算法 [Asa96] を教えていただいた. 早速実装実験し, 本稿の手法との比較を検討中である.

[3] Risa/Asir は分散処理のための通信機能を備えている.

参 考 文 献

[Asa96] 浅井 哲也, "Borcherdsの無限積-入門一歩手前", 第41回代数学シンポジウム報告集, (1996), pp.113-122.

[Ito95] Hideji ITO, "Computation of the Modular Equation", *Proc.Japan Acad.*, 71A, pp.48-50(1995),

[Kog97] 小暮 淳, "Schoofアルゴリズム (楕円曲線上有理点個数の計算) のRisa/Asirによる実装", 数式処理における理論と応用の研究, (1998).

[La87] Serge Lang, "Elliptic Functions(Second Edition)", *Graduate Texts in Mathematics*, 112(1987), Springer-Verlag.

[Sc85] Schoof, R., "Elliptic curves over finite fields and the computation of square roots mod p", *Mathematics of Computation*, 44(1985), pp.483-494.

[Sc95] Schoof, R., "Counting points on elliptic curves over finite fields", *Journal de Theorie des Nombres de Bordeaux*, 7(1995), pp.219-254.

付録

$l = 2, 3, 5, 7, 11, 13$ に対するモジュラー多項式の係数を挙げる. ただし

$$\Phi_l(X, j) = X^{l+1} + j^{l+1} + \sum_{m,n=0}^{l} a_{m,n} X^m j^n$$

である.

● $l = 2$

$$\begin{aligned}
a_{0,0} &= -2^{12} \cdot 3^9 \cdot 5^9 \\
a_{1,0} = a_{0,1} &= +2^8 \cdot 3^7 \cdot 5^6 \\
a_{1,1} &= +3^4 \cdot 5^3 \cdot 4027 \\
a_{2,0} = a_{0,2} &= -2^4 \cdot 3^4 \cdot 5^3 \\
a_{2,1} = a_{1,2} &= +2^4 \cdot 3 \cdot 31 \\
a_{2,2} &= -1
\end{aligned}$$

● $l = 3$

$$\begin{aligned}
a_{0,0} &= 0 \\
a_{1,0} = a_{0,1} &= +2^{45} \cdot 3^3 \cdot 5^9 \\
a_{1,1} &= -2^{31} \cdot 5^6 \cdot 22973 \\
a_{2,0} = a_{0,2} &= +2^{30} \cdot 3^3 \cdot 5^6 \\
a_{2,1} = a_{1,2} &= +2^{16} \cdot 3^5 \cdot 5^3 \cdot 17 \cdot 263 \\
a_{2,2} &= +2 \cdot 3^4 \cdot 13 \cdot 193 \cdot 6367 \\
a_{3,0} = a_{0,3} &= +2^{15} \cdot 3^2 \cdot 5^3 \\
a_{3,1} = a_{1,3} &= -2^2 \cdot 3^3 \cdot 9907
\end{aligned}$$

$$a_{3,2} = a_{2,3} = +2^3 \cdot 3^2 \cdot 31$$
$$a_{3,3} = -1$$

● $l = 5$

$$a_{0,0} = +2^{90} \cdot 3^{18} \cdot 5^3 \cdot 11^9$$
$$a_{1,0} = a_{0,1} = +2^{77} \cdot 3^{16} \cdot 5^3 \cdot 11^6 \cdot 31 \cdot 1193$$
$$a_{1,1} = -2^{62} \cdot 3^{13} \cdot 11^3 \cdot 26984268714163$$
$$a_{2,0} = a_{0,2} = +2^{60} \cdot 3^{13} \cdot 5^2 \cdot 11^3 \cdot 13^2 \cdot 3167 \cdot 204437$$
$$a_{2,1} = a_{1,2} = +2^{47} \cdot 3^{10} \cdot 5^4 \cdot 53359 \cdot 131896604713$$
$$a_{2,2} = +2^{30} \cdot 3^8 \cdot 5^4 \cdot 7 \cdot 13 \cdot 1861 \cdot 6854302120759$$
$$a_{3,0} = a_{0,3} = +2^{48} \cdot 3^9 \cdot 5^2 \cdot 31 \cdot 1193 \cdot 24203 \cdot 2260451$$
$$a_{3,1} = a_{1,3} = -2^{31} \cdot 3^7 \cdot 5^3 \cdot 327828841654280269$$
$$a_{3,2} = a_{2,3} = +2^{17} \cdot 3^4 \cdot 5^3 \cdot 2311 \cdot 2579 \cdot 3400725958453$$
$$a_{3,3} = -2^2 \cdot 5^2 \cdot 11 \cdot 17 \cdot 131 \cdot 1061 \cdot 169751677267033$$
$$a_{4,0} = a_{0,4} = +2^{30} \cdot 3^7 \cdot 5 \cdot 13^2 \cdot 3167 \cdot 204437$$
$$a_{4,1} = a_{1,4} = +2^{20} \cdot 3^4 \cdot 5^3 \cdot 12107359229837$$
$$a_{4,2} = a_{2,4} = +3 \cdot 5^3 \cdot 167 \cdot 6117103549378223$$
$$a_{4,3} = a_{3,4} = +2^5 \cdot 3 \cdot 5^2 \cdot 197 \cdot 227 \cdot 421 \cdot 2387543$$
$$a_{4,4} = +2^3 \cdot 5^2 \cdot 257 \cdot 32412439$$
$$a_{5,0} = a_{0,5} = +2^{17} \cdot 3^4 \cdot 5 \cdot 31 \cdot 1193$$
$$a_{5,1} = a_{1,5} = -2 \cdot 3 \cdot 5^2 \cdot 1644556073$$
$$a_{5,2} = a_{2,5} = +2^5 \cdot 5^2 \cdot 13 \cdot 195053$$
$$a_{5,3} = a_{3,5} = -2^2 \cdot 3^2 \cdot 5 \cdot 131 \cdot 193$$
$$a_{5,4} = a_{4,5} = +2^3 \cdot 3 \cdot 5 \cdot 31$$
$$a_{5,5} = -1$$

● $l = 7$

$$a_{0,0} = 0$$
$$a_{1,0} = a_{0,1} = 0$$
$$a_{1,1} = +2^{91} \cdot 3^{27} \cdot 5^{18} \cdot 11 \cdot 13 \cdot 17^9$$
$$a_{2,0} = a_{0,2} = +2^{90} \cdot 3^{27} \cdot 5^{18} \cdot 7^3 \cdot 17^9$$
$$a_{2,1} = a_{1,2} = -2^{76} \cdot 3^{25} \cdot 5^{15} \cdot 7^2 \cdot 17^7 \cdot 947 \cdot 22541$$
$$a_{2,2} = -2^{61} \cdot 3^{20} \cdot 5^{12} \cdot 7^2 \cdot 17^3 \cdot 1644361 \cdot 60057292681$$
$$a_{3,0} = a_{0,3} = +2^{76} \cdot 3^{25} \cdot 5^{15} \cdot 7^3 \cdot 17^6 \cdot 31 \cdot 26891$$
$$a_{3,1} = a_{1,3} = -2^{61} \cdot 3^{19} \cdot 5^{12} \cdot 7^2 \cdot 17^3 \cdot 19 \cdot 487 \cdot 88980809456419$$
$$a_{3,2} = a_{2,3} = +2^{46} \cdot 3^{16} \cdot 5^9 \cdot 7^2 \cdot 409 \cdot 2633 \cdot 231491957605001610911$$
$$a_{3,3} = -2^{31} \cdot 3^{10} \cdot 5^6 \cdot 7^2 \cdot 23131 \cdot 216217 \cdot 50485308001 \cdot 220185774353$$
$$a_{4,0} = a_{0,4} = +2^{60} \cdot 3^{19} \cdot 5^{12} \cdot 7^2 \cdot 17^3 \cdot 397 \cdot 1323331291097$$
$$a_{4,1} = a_{1,4} = +2^{46} \cdot 3^{17} \cdot 5^9 \cdot 7^2 \cdot 13 \cdot 12983 \cdot 3769379869638077087$$

$$a_{4,2} = a_{2,4} = +2^{31} \cdot 3^{11} \cdot 5^6 \cdot 7^2 \cdot 17 \cdot 10291297 \cdot 6058491976028534574607$$
$$a_{4,3} = a_{3,4} = +2^{16} \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 37 \cdot 43 \cdot 661 \cdot 350674256651 \cdot 11102596733852951$$
$$a_{4,4} = +2 \cdot 5 \cdot 7^2 \cdot 197 \cdot 47159882113 \cdot 6729443099 \cdot 2873772276642577$$
$$a_{5,0} = a_{0,5} = +2^{47} \cdot 3^16 \cdot 5^9 \cdot 7^2 \cdot 13 \cdot 31 \cdot 26891 \cdot 683503 \cdot 9854261$$
$$a_{5,1} = a_{1,5} = -2^{33} \cdot 3^11 \cdot 5^6 \cdot 7^2 \cdot 3697 \cdot 9447061867111661492633$$
$$a_{5,2} = a_{2,5} = +2^{19} \cdot 3^9 \cdot 5^3 \cdot 7^2 \cdot 4182301 \cdot 9596669941 \cdot 4442354862109$$
$$a_{5,3} = a_{3,5} = -2^3 \cdot 7^2 \cdot 1523 \cdot 950447 \cdot 152027963 \cdot 10451975377800026969$$
$$a_{5,4} = a_{4,5} = +2^5 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 113 \cdot 41659 \cdot 85554840812719128607$$
$$a_{5,5} = -2^2 \cdot 3^2 \cdot 7^2 \cdot 1766872571 \cdot 5871738041631817$$
$$a_{6,0} = a_{0,6} = +2^{30} \cdot 3^10 \cdot 5^6 \cdot 7 \cdot 397 \cdot 1323331291097$$
$$a_{6,1} = a_{1,6} = +2^{17} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 59 \cdot 10020909155496489683$$
$$a_{6,2} = a_{2,6} = +2^2 \cdot 7^2 \cdot 29 \cdot 1291 \cdot 6221 \cdot 22317853 \cdot 10487936253649$$
$$a_{6,3} = a_{3,6} = +2^4 \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 197 \cdot 227 \cdot 2113 \cdot 2087377 \cdot 85827811$$
$$a_{6,4} = a_{4,6} = +2^3 \cdot 3 \cdot 7^2 \cdot 302587 \cdot 12536290128459761$$
$$a_{6,5} = a_{5,6} = +2^4 \cdot 7^3 \cdot 3259 \cdot 9901340156731$$
$$a_{6,6} = +3^2 \cdot 7^2 \cdot 13 \cdot 67 \cdot 97 \cdot 8389943$$
$$a_{7,0} = a_{0,7} = +2^{16} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 31 \cdot 26891$$
$$a_{7,1} = a_{1,7} = -2^3 \cdot 7^2 \cdot 13 \cdot 2129 \cdot 5107 \cdot 631559$$
$$a_{7,2} = a_{2,7} = +2^4 \cdot 3^4 \cdot 7^2 \cdot 43 \cdot 1801 \cdot 146437$$
$$a_{7,3} = a_{3,7} = -2 \cdot 3 \cdot 7^2 \cdot 13 \cdot 1067425727$$
$$a_{7,4} = a_{4,7} = +2^5 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 43 \cdot 509$$
$$a_{7,5} = a_{5,7} = -2^2 \cdot 3^3 \cdot 7 \cdot 13553$$
$$a_{7,6} = a_{6,7} = +2^3 \cdot 3 \cdot 7 \cdot 31$$
$$a_{7,7} = -1$$

● $l = 11$

$$a_{0,0} = +2^{189} \cdot 3^{36} \cdot 5^{36} \cdot 11^3 \cdot 17^9 \cdot 29^9$$
$$a_{1,0} = a_{0,1} = -2^{171} \cdot 3^{34} \cdot 5^{34} \cdot 11^3 \cdot 17^6 \cdot 29^6 \cdot 41 \cdot 2339 \cdot 69644987$$
$$a_{1,1} = +2^{153} \cdot 3^{31} \cdot 5^{31} \cdot 17^3 \cdot 29^3 \cdot 139 \cdot 487 \cdot 26094174253158533018911091$$
$$a_{2,0} = a_{0,2} = +2^{153} \cdot 3^{31} \cdot 5^{33} \cdot 7 \cdot 11^3 \cdot 17^3 \cdot 29^3 \cdot 4782100987 \cdot 344312460241097$$
$$a_{2,1} = a_{1,2} = -2^{135} \cdot 3^{28} \cdot 5^{30} \cdot 11^2 \cdot 847672369 \cdot 99653077165199 \cdot 440177210954005013$$
$$a_{2,2} = -2^{121} \cdot 3^{27} \cdot 5^{24} \cdot 11^2 \cdot 79 \cdot 37501426316689$$
$$\cdot 6968668849798489758082691399 17$$
$$a_{3,0} = a_{0,3} = -2^{135} \cdot 3^{27} \cdot 5^{29} \cdot 11^3 \cdot 373 \cdot 3559 \cdot 13091471$$
$$\cdot 2358397924764491602215171 53$$
$$a_{3,1} = a_{1,3} = +2^{122} \cdot 3^{26} \cdot 5^{25} \cdot 11^2 \cdot 13 \cdot 17 \cdot 192187 \cdot 380732888279$$
$$\cdot 6265047708142861167947863 1$$
$$a_{3,2} = a_{2,3} = +2^{105} \cdot 3^{23} \cdot 5^{22} \cdot 11^2 \cdot 31 \cdot 61$$
$$\cdot 3895565096545306837 \cdot 12798372181436485278730926 6167$$

$$a_{3,3} = -2^{92}\cdot 3^{19}\cdot 5^{19}\cdot 11^2\cdot 17\cdot 263\cdot 887\cdot 1861 \cdot 944071276590326279738709985592072024289202157 3$$

$$a_{4,0} = a_{0,4} = +2^{120}\cdot 3^{26}\cdot 5^{24}\cdot 11^2\cdot 44449 \cdot 4035968409530076961073771011198728413071 3$$

$$a_{4,1} = a_{1,4} = +2^{105}\cdot 3^{23}\cdot 5^{22}\cdot 11^2\cdot 5119\cdot 1010509\cdot 107477479 \cdot 9740331807284708306333829387825 1$$

$$a_{4,2} = a_{2,4} = +2^{92}\cdot 3^{20}\cdot 5^{19}\cdot 11^2\cdot 167\cdot 43936132389613\cdot 1209892575072298417 \cdot 1069978044470171814391$$

$$a_{4,3} = a_{3,4} = -2^{75}\cdot 3^{17}\cdot 5^{17}\cdot 7^2\cdot 11^2\cdot 413887\cdot 1301033\cdot 2101344104207 \cdot 72494103160331\cdot 28193421923025791633$$

$$a_{4,4} = +2^{61}\cdot 3^{14}\cdot 5^{12}\cdot 11^2\cdot 13\cdot 71^2\cdot 947\cdot 1237013\cdot 5220865967773243033 \cdot 1152038815155973497035530414423 31$$

$$a_{5,0} = a_{0,5} = -2^{107}\cdot 3^{23}\cdot 5^{22}\cdot 7\cdot 11^2\cdot 61\cdot 2081\cdot 26387\cdot 631025971 \cdot 477187215399935968050495793 87$$

$$a_{5,1} = a_{1,5} = -2^{91}\cdot 3^{20}\cdot 5^{19}\cdot 11^2\cdot 71\cdot 177657338534510117 \cdot 3119790401602336843918431304632 2933$$

$$a_{5,2} = a_{2,5} = +2^{76}\cdot 3^{18}\cdot 5^{19}\cdot 11^2\cdot 499\cdot 24850220882830656594473 \cdot 1160045526825664189083366414 2227$$

$$a_{5,3} = a_{3,5} = -2^{64}\cdot 3^{14}\cdot 5^{12}\cdot 11^2\cdot 3673\cdot 126493901\cdot 11221329683 \cdot 9780148349891017115171329367145801 4959169$$

$$a_{5,4} = a_{4,5} = -2^{47}\cdot 3^{11}\cdot 5^{10}\cdot 11^2\cdot 63913 \cdot 945341478950774382480174982314766888646035878547510465412 40941$$

$$a_{5,5} = -2^{33}\cdot 3^{9}\cdot 5^{7}\cdot 7^2\cdot 11^2 \cdot 192262416122548321953137134772767570206376697307986458387807452615953$$

$$a_{6,0} = a_{0,6} = +2^{92}\cdot 3^{19}\cdot 5^{20}\cdot 11^2\cdot 53\cdot 42821 \cdot 6326560515992477973789309049539998204602660 43$$

$$a_{6,1} = a_{1,6} = -2^{75}\cdot 3^{17}\cdot 5^{17}\cdot 11^2\cdot 152767\cdot 1099289\cdot 9086229100183 \cdot 1387182922130054215221145625404 69$$

$$a_{6,2} = a_{2,6} = +2^{60}\cdot 3^{14}\cdot 5^{12}\cdot 11^2\cdot 13\cdot 31\cdot 20323\cdot 8252819536542092276536799 \cdot 2769472684395627390588360581903$$

$$a_{6,3} = a_{3,6} = -2^{45}\cdot 3^{10}\cdot 5^{10}\cdot 11^2\cdot 13\cdot 191\cdot 349\cdot 373783\cdot 1418959\cdot 1627537 \cdot 12895556201217577\cdot 30453708279021328666887383 3$$

$$a_{6,4} = a_{4,6} = +2^{30}\cdot 3^{8}\cdot 5^{7}\cdot 11^2\cdot 41\cdot 269\cdot 1429\cdot 29392360673478679616774272 3 \cdot 6284504830515359093735967706276937747$$

$$a_{6,5} = a_{5,6} = +2^{19}\cdot 3^{5}\cdot 5^{5}\cdot 7\cdot 11^2\cdot 127\cdot 18905749\cdot 913095473 \cdot 3030961705348554262466221233573114967218017001540676 97$$

$$a_{6,6} = +2^{2}\cdot 3\cdot 7\cdot 11^2\cdot 641\cdot 10560541 \cdot 1697812875269522893667639490397278096675870058265318463551941037331 1$$

$$a_{7,0} = a_{0,7} = +2^{76}\cdot 3^{17}\cdot 5^{17}\cdot 11^2\cdot 7049164663\cdot 25303350811 \cdot 3851649398722576824137367979487$$

$$
\begin{aligned}
a_{7,1} &= a_{1,7} = -2^{62}\cdot 3^{14}\cdot 5^{12}\cdot 11^2\cdot 31\cdot 37\cdot 10247294251\cdot 201775666927\\
&\quad\cdot 156314806130331598368124285761165 61\\
a_{7,2} &= a_{2,7} = +2^{48}\cdot 3^{11}\cdot 5^{10}\cdot 11^2\cdot 41\cdot 607102549518110772774820 3399\\
&\quad\cdot 304663350316385610961153359445 4501\\
a_{7,3} &= a_{3,7} = -2^{31}\cdot 3^8\cdot 5^7\cdot 11^2\cdot 17\cdot 61\cdot 3371\cdot 6397\cdot 25875251350825859\\
&\quad\cdot 124576517163808499\\
&\quad\cdot 230117514815823797783872\\
a_{7,4} &= a_{4,7} = +2^{16}\cdot 3^5\cdot 5^5\cdot 11^2\cdot 307\cdot 1669\cdot 350443\cdot 4860763483186908824719\\
&\quad\cdot 565684401192362579948438270961670506097\\
a_{7,5} &= a_{5,7} = -2^3\cdot 3^2\cdot 11^2\cdot 23\cdot 355941022551001\cdot 931466000922959\\
&\quad\cdot 114321768472858074343169715967366671310585 3363\\
a_{7,6} &= a_{6,7} = +2^4\cdot 3^2\cdot 5^2\cdot 11^2\cdot 29\cdot 323944031\\
&\quad\cdot 60578858409691552283165292712318720178329149543086981728681\\
a_{7,7} &= -2\cdot 3\cdot 5\cdot 7\cdot 11^2\cdot 13\cdot 2530201\cdot 8742888084290482628997121\\
&\quad\cdot 889506295397596454306670993691 7\\
a_{8,0} &= a_{0,8} = +2^{61}\cdot 3^{14}\cdot 5^{12}\cdot 11\cdot 661\cdot 15809\cdot 5059767481605304433137\\
&\quad\cdot 854771338417349922521177\\
a_{8,1} &= a_{1,8} = +2^{45}\cdot 3^{11}\cdot 5^{10}\cdot 11^2\cdot 13\cdot 515515654543736004997\\
&\quad\cdot 135351545092790255821644358728151 3337\\
a_{8,2} &= a_{2,8} = +2^{30}\cdot 3^9\cdot 5^8\cdot 11^2\cdot 19\cdot 113\cdot 21149\\
&\quad\cdot 37873943798951170112098696725551576898244671602043648 11\\
a_{8,3} &= a_{3,8} = +2^{15}\cdot 3^5\cdot 5^6\cdot 11^2\cdot 37\cdot 179\cdot 3217\cdot 17207\cdot 146681\\
&\quad\cdot 98218443554449139940009024126132915666050255477269\\
a_{8,4} &= a_{4,8} = +3^2\cdot 5\cdot 11^2\cdot 137\cdot 239\cdot 8243\cdot 7887026866401228121\\
&\quad\cdot 6105340823860024647 41\cdot 1200929269524023002196339\\
a_{8,5} &= a_{5,8} = +2^5\cdot 3\cdot 5^2\cdot 11^2\cdot 13\cdot 54300886385547330571636959227\\
&\quad\cdot 101628077124044298794771650243438 7633\\
a_{8,6} &= a_{6,8} = +2^3\cdot 3^3\cdot 5\cdot 11^2\cdot 191\cdot 19460723\cdot 36547573\\
&\quad\cdot 55643244512293624465622423709673718339644003\\
a_{8,7} &= a_{7,8} = +2^5\cdot 3^2\cdot 5\cdot 11^2\cdot 13\cdot 43\cdot 16505907668687\cdot 50672045811913\\
&\quad\cdot 7817666684765906771160053\\
a_{8,8} &= +2\cdot 3\cdot 11^2\cdot 73\cdot 1069\cdot 57653\cdot 101377\cdot 44358911\\
&\quad\cdot 19887019565263255499001003 49\\
a_{9,0} &= a_{0,9} = +2^{47}\cdot 3^9\cdot 5^{10}\cdot 11\cdot 523\\
&\quad\cdot 62013601680795547941547763247812546240058393179 83\\
a_{9,1} &= a_{1,9} = -2^{31}\cdot 3^7\cdot 5^7\cdot 7\cdot 11^2\cdot 47\cdot 9391\cdot 35281\cdot 24414359329\\
&\quad\cdot 75190698535714297\cdot 164133976635704323\\
a_{9,2} &= a_{2,9} = +2^{16}\cdot 3^4\cdot 5^5\cdot 11^2\cdot 37\cdot 307\cdot 1423\cdot 14537\cdot 286041091279\\
&\quad\cdot 59627028354672589328107703381330 31079\\
a_{9,3} &= a_{3,9} = -2^2\cdot 5\cdot 7\cdot 11^2\cdot 73\cdot 97\cdot 631\cdot 16673\cdot 6834495353622748907
\end{aligned}
$$

$$\cdot 230943953459394635537173837202065 93$$

$$a_{9,4} = a_{4,9} = +2^5 \cdot 3^2 \cdot 5^3 \cdot 11^2 \cdot 101527 \cdot 263395087 \cdot 2771391563 \cdot 6860709708136455151155 0047755018111$$

$$a_{9,5} = a_{5,9} = -2^2 \cdot 3^2 \cdot 5 \cdot 11^2 \cdot 23 \cdot 127 \cdot 58196209 \cdot 178221271391329 \cdot 564068543478079 \cdot 2672694011855719$$

$$a_{9,6} = a_{6,9} = +2^4 \cdot 5 \cdot 11^2 \cdot 37 \cdot 103 \cdot 1511 \cdot 6173 \cdot 426933638895430592108653461013745967799 51$$

$$a_{9,7} = a_{7,9} = -2^2 \cdot 3 \cdot 5^3 \cdot 11^2 \cdot 17 \cdot 73 \cdot 110285960469101 \cdot 205850183814633362086812 4147$$

$$a_{9,8} = a_{8,9} = +2^3 \cdot 3^2 \cdot 11^2 \cdot 29 \cdot 95898615266887459564667829595002797749$$

$$a_{9,9} = -11^2 \cdot 23 \cdot 107 \cdot 347 \cdot 827449275119 \cdot 6706274535671189$$

$$a_{10,0} = a_{0,10} = +2^{32} \cdot 3^7 \cdot 5^8 \cdot 11 \cdot 41 \cdot 7023569081983 \cdot 2520808278821983693$$

$$a_{10,1} = a_{1,10} = +2^{16} \cdot 3^4 \cdot 5^5 \cdot 7 \cdot 11^2 \cdot 53 \cdot 787 \cdot 25765639 \cdot 29092430490503 \cdot 76134299273803$$

$$a_{10,2} = a_{2,10} = +2 \cdot 3 \cdot 11^2 \cdot 173 \cdot 19919 \cdot 204297207020280290909 \cdot 3106443453542672791477$$

$$a_{10,3} = a_{3,10} = +2^3 \cdot 3^2 \cdot 5^2 \cdot 11^2 \cdot 13 \cdot 41 \cdot 97 \cdot 313 \cdot 400943691425850890698895728587814 0697$$

$$a_{10,4} = a_{4,10} = +2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 163 \cdot 3041 \cdot 639329 \cdot 6264328687 \cdot 175306121994039044807$$

$$a_{10,5} = a_{5,10} = +2^4 \cdot 3 \cdot 5 \cdot 11^2 \cdot 83 \cdot 4937 \cdot 144701 \cdot 167782389645652534502586635 99$$

$$a_{10,6} = a_{6,10} = +3 \cdot 11^2 \cdot 53003 \cdot 484037 \cdot 84275256818445278610759511 9$$

$$a_{10,7} = a_{7,10} = +2^4 \cdot 5 \cdot 7^2 \cdot 11^3 \cdot 89 \cdot 23609 \cdot 58876895419733991550837$$

$$a_{10,8} = a_{8,10} = +2^4 \cdot 3 \cdot 11^2 \cdot 2857 \cdot 17921963 \cdot 41722683520915207$$

$$a_{10,9} = a_{9,10} = +2^6 \cdot 3^2 \cdot 7 \cdot 11^3 \cdot 59 \cdot 313 \cdot 304071601918951$$

$$a_{10,10} = +2 \cdot 3 \cdot 7 \cdot 11^2 \cdot 137 \cdot 2310043787617$$

$$a_{11,0} = a_{0,11} = +2^15 \cdot 3^4 \cdot 5^5 \cdot 11 \cdot 29 \cdot 547 \cdot 33529 \cdot 6109399$$

$$a_{11,1} = a_{1,11} = -2^2 \cdot 3 \cdot 7 \cdot 11^2 \cdot 13 \cdot 2835361656197600834891$$

$$a_{11,2} = a_{2,11} = +2^3 \cdot 5^2 \cdot 11^2 \cdot 863 \cdot 1302864869715323531$$

$$a_{11,3} = a_{3,11} = -3^2 \cdot 5 \cdot 11^2 \cdot 47 \cdot 83 \cdot 2753 \cdot 9048702577427$$

$$a_{11,4} = a_{4,11} = +2^6 \cdot 3 \cdot 5 \cdot 11^2 \cdot 23 \cdot 67 \cdot 1777 \cdot 18959 \cdot 712669$$

$$a_{11,5} = a_{5,11} = -2^3 \cdot 11^2 \cdot 23 \cdot 12063301 \cdot 66645707$$

$$a_{11,6} = a_{6,11} = +2^4 \cdot 3^2 \cdot 11^2 \cdot 1116653 \cdot 2187971$$

$$a_{11,7} = a_{7,11} = -2 \cdot 3 \cdot 5 \cdot 11 \cdot 185027238353$$

$$a_{11,8} = a_{8,11} = +2^5 \cdot 11 \cdot 3457 \cdot 44119$$

$$a_{11,9} = a_{9,11} = -2^2 \cdot 3^2 \cdot 11 \cdot 71411$$

$$a_{11,10} = a_{10,11} = +2^3 \cdot 3 \cdot 11 \cdot 31$$

$$a_{11,11} = -1$$